In the Specification

Please delete paragraph 00012 and substitute the following paragraph therefor:

[00012] In another embodiment, the present invention is directed to a method for protecting a computer network comprised of a plurality of computer systems and a client remediation server for resolving vulnerabilities in the plurality of computer systems. In accordance with the claimed method, exchanges between the remediated computer network and a computer system thereof are temporarily limited whenever the computer system is disconnected from the remediated computer network and subsequently reconnected thereto. Preferably, exchanges between the remediated computer network and the computer system are limited until after the client remediation server has checked for pending remediations for the computer system and all such pending remediations have been executed. A firewall may be used to limit exchanges between the computer system and the remediated computer network. The firewall is raised upon reconnection of the computer system to the remediated computer network. Once raised, the firewall filters out non-remediation-related traffic between the computer system and the remediated computer network. The limitations on exchanges between the computer system and the remediated computer network are removed as soon as the client remediation server has provided the information needed for an agent, residing on the computer system, to execute the pending ~~remediations~~ <u>remediations.</u> To remove the limitations on exchanges between the computer system and the remediated computer network, the computer system lowers the firewall previously raised, by the computer system, on reconnection of the computer system with the remediated computer network. Once the limitations on exchanges between the

computer system and the remediated computer network have been removed, non-remediation-related traffic is able to pass between the computer system and the remediated computer network.

Please delete paragraph 00031 and substitute the following paragraph therefor:

[00031] As will be more fully described below, the central remediation server 12 provides remediation services to one or more computer networks, for example, computer network 19, coupled to the central remediation server 12 by a web server 20, for example, a VFLASH server. Of course, for ease of illustration, only one such computer network is shown in FIG. 1. If additional computer networks were to receive remediation services [[form]] <u>from</u> the central remediation server 12, all such additional computer networks would also be coupled to the central remediation server 12 by the VFLASH server 20. Additional VFLASH servers would be necessary only when the demand for remediation services is sufficiently heavy that the additional computer networks can no longer timely download remediation signatures from the VFLASH server 20. Variously, it is contemplated that the computer network 19 may be a LAN, wide area network (WAN), wireless LAN (WLAN), virtual private network (VPN), wireless VPN (WVPN) or the Internet. Of course, the foregoing list is not intended to be exhaustive and it is fully contemplated that other types of computer network would be suitable for the purposes contemplated herein.

Please delete paragraph 00033 and substitute the following paragraph therefor:

[0001] It should be clearly understood that the computer network 19 has been ~~greater~~ greatly simplified for ease of description. For example, in FIG. 1, various types of devices, for example, routers, switches, and printers, which typically form part of a computer network, have been omitted from the drawing. FIG. 1 also shows the computer network 19 as including only a single client remediation server, specifically, the client remediation server 22. It should be clearly understood that, depending on the configuration of the computer network 19, additional client remediation servers may be required. Of course, when plural client remediation servers are required, each such client remediation server should be coupled to the client administration console 25 in a manner similar to that illustrated with respect to the client remediation server 22. Also, FIG. 1 shows each one of the file servers 26a, PCs 26b and portable computers 26c as being directly coupled to the client remediation server 22. However, depending on the particular configuration of the computer network 19, one or more of these devices may instead be indirectly coupled to the client remediation server 22, typically, through another network device. For example, a PC may be coupled to the client remediation server 22 through a file server. Finally, the interconnections between the various ones of the network devices such as the file servers 26a, the PCs 26b and the portable computers 26c of the computer network 19 have been omitted from FIG. 1 for ease of description.

Please delete paragraph 00045 and substitute the following paragraph therefor:

[00045] Residing on the processor subsystem 160 are a remediation agent 163, a first (or local) application 164, a second (or network protection initialization) application 166, a third (or network interface) application 168 and a fourth (or firewall) application 170. The remediation agent 163 and each of the applications 164 through 170 are respectively comprised of a series of encoded instructions which reside in the memory subsystem 162 and are executable by the processor subsystem 160. Also residing in the memory subsystem 162 are plural types of information. Each type of information may be stored at plural locations within the memory subsystem 162 which are associated with one another or, as illustrated in FIG. [[6]] 2, the memory subsystem 162 may be subdivided into plural memory areas, each of which maintains a specified type of information. For example, the memory subsystem 162 includes a first memory area 172 in which initialization information is maintained, a second memory area 174 in which local application data is maintained and a third memory area 176 in which a set of disconnected machine rules is maintained.

Please delete paragraph 00047 and substitute the following paragraph therefor:

[00047] While the network interface application 168 provides the interface between the various applications, specifically, the local application 164, the remediation agent [[165]] 163 and the network protection initialization application 166, of the disconnected computer system 26c to the remediated computer network 19, it is the implementation of a firewall that enables the disconnected computer system 26c to periodically quarantine itself from the remediated computer network 19, for example, when the

disconnected computer system 26c seeks to re-connect with the remediated computer network 19. While firewalls may be implemented in either hardware or software, FIG. 1 shows a software-implemented firewall, specifically, the firewall application 170. The firewall application 170 works by limiting the flow of traffic between the network interface application 168 and the network interface applications of the various devices which collectively form the remediated computer network 19, for example, a network interface application 186 of client remediation server 22. The firewall application 170 is switchable between first and second states. In the first state, the firewall would be considered as being in a closed position in which traffic to and/or from the disconnected computer system 26c is limited while, in the second state, the firewall would be considered as being in an open condition in which traffic to and/or from the disconnected computer system 26c is unrestricted. Finally, when in the closed position, traffic between the disconnected computer system 26c and the client remediation server 22 is typically limited to (1) signals identifying the client remediation server 22 and/or the disconnected computer system 26c; and (2) signals containing remediation signatures.

Please delete paragraph 00048 and substitute the following paragraph therefor:

[00048] The client remediation server 22 includes a processor subsystem 180, for example, a CPU, coupled to a memory subsystem 182 by a system bus (not shown). As disclosed herein, the processor subsystem 180 represents the collective processing functionality of the ~~disconnected computer system 22c~~ <u>client remediation server 22</u> and may be distributed amongst any number of processing devices. Similarly, the memory

subsystem 182 represents the collective storage functionality of the ~~disconnected computer system~~ client remediation server 22 and, like the processor subsystem 180, may be distributed amongst any number of memory devices. Residing on the processor subsystem 180 are a first (or remediation) application 184 and a second (or network interface) application 186. The first and second applications 184 and 186 are each comprised of a series of encoded instructions which reside in the memory subsystem 182 and are executable by the processor subsystem 180. As will be more fully described below, the remediation application 184 provides remediation signatures to the remediation agent 163 for use in resolving vulnerabilities for the disconnected computer system 26c. Also residing in the memory subsystem 182 are plural types of information. Each type of information may be stored at plural locations within the memory subsystem 182 which are associated with one another or the memory subsystem 182 may be subdivided into plural memory areas, each of which maintains a specified type of information. For example, the memory subsystem 182 includes a first memory area 188 in which remediation profiles are maintained, a second memory area 190 in which vulnerability information is maintained, a third memory area 192 in which remediation signatures are maintained and a fourth memory area 194 in which initialization information is maintained.

Please delete paragraph 00054 and substitute the following paragraph therefor:

[00054] Proceeding on to step 57, the scheduled remediations of the computer systems 26a, 26b and 26c of the computer network 19 are performed. To perform the remediations, the client remediation server 22 delivers the appropriate remediation

signature to a computer system, for example, the computer system 26c. There, the remediation signature is executed by the remediation agent 165, thereby resolving the vulnerabilities of [[he]] <u>the</u> computer system 26c. Upon completion of the scheduled remediation at step 57, the method proceeds to step 58 for review of the completed remediation. For example, status reports or other reporting tools may be used by the client remediation server 22 to determine if the scheduled remediation was successfully completed. In addition, remediation events may be logged or otherwise recorded to preserve information related to the completed remediation. Such information may be included in profiles for the computer systems 26a, 26b, 26c residing at the client remediation server 22. As previously noted, such profiles may include information about the remediated computer systems such as system configuration, software, and prior remediation actions or a remediation history. Having such information allows for managed remediation of the computer systems 26a, 26b, and 26c. After reviewing the completed remediation at step 58, the method ends at step 59.

Please delete paragraph 00057 and substitute the following paragraph therefor:

[00057] Continuing on to step 72, a remediation profile is then generated for each target, for example, the portable computer 26c, and stored in the remediation profile area 188. As noted, each remediation profile typically includes information regarding the vulnerabilities identified on the target client computer as well as the corresponding signatures to address those vulnerabilities. At step 74, the client administrator, typically an IT person or other computer security personnel, is given the opportunity to select which vulnerabilities should be remediated. Generally, the selection is made by

reviewing the information regarding vulnerabilities, proposed signatures, and profiles maintained in the remediation profile area [[72.]] 188. The selection and review may be made for each computer or by vulnerability. For example, a particular computer could be selected not to receive any remediation, perhaps because the computer does not pose a significant security risk, the vulnerabilities on the computer are not significant, the processes running on the computer cannot be interrupted for remediation, etc. Alternatively, a particular vulnerability could be deselected for all target client computers, such that the vulnerability would not be remediated on any of the target computers, perhaps because the vulnerability does not pose a sufficient security risk, the remediation signature is deemed too risky, etc. The review process could also include a compliance check in which target computers are checked for compliance with the proposed remediation. For example, while the remediation signature for a target computer may include the installation of a patch, a compliance check may reveal that the patch is already installed on the target computer.